Cybersecurity
Network Security Protocols

Kasun De Zoysa

Department of Communication and Media Technologies
University of Colombo School of Computing
University of Colombo
Sri Lanka

Network Security Protocols

- Network-related security protocols in common use include:
- **Transport Layer Security (TLS):** Used extensively on the web and is often referred to in privacy policies as a means of providing confidential web connections.
- **Secure Shell (SSH):** Used for remote login, file transfer, and limited VPN service.
- **IP Security (IPsec):** Provides security services at the IP level and is used to provide Virtual Private Network (VPN) services.
- **WiFi security (WEP, WPA, WPA2):** Provides security services at the link layer for wireless communication
- DNS Security Protocol **(DNSSec)**

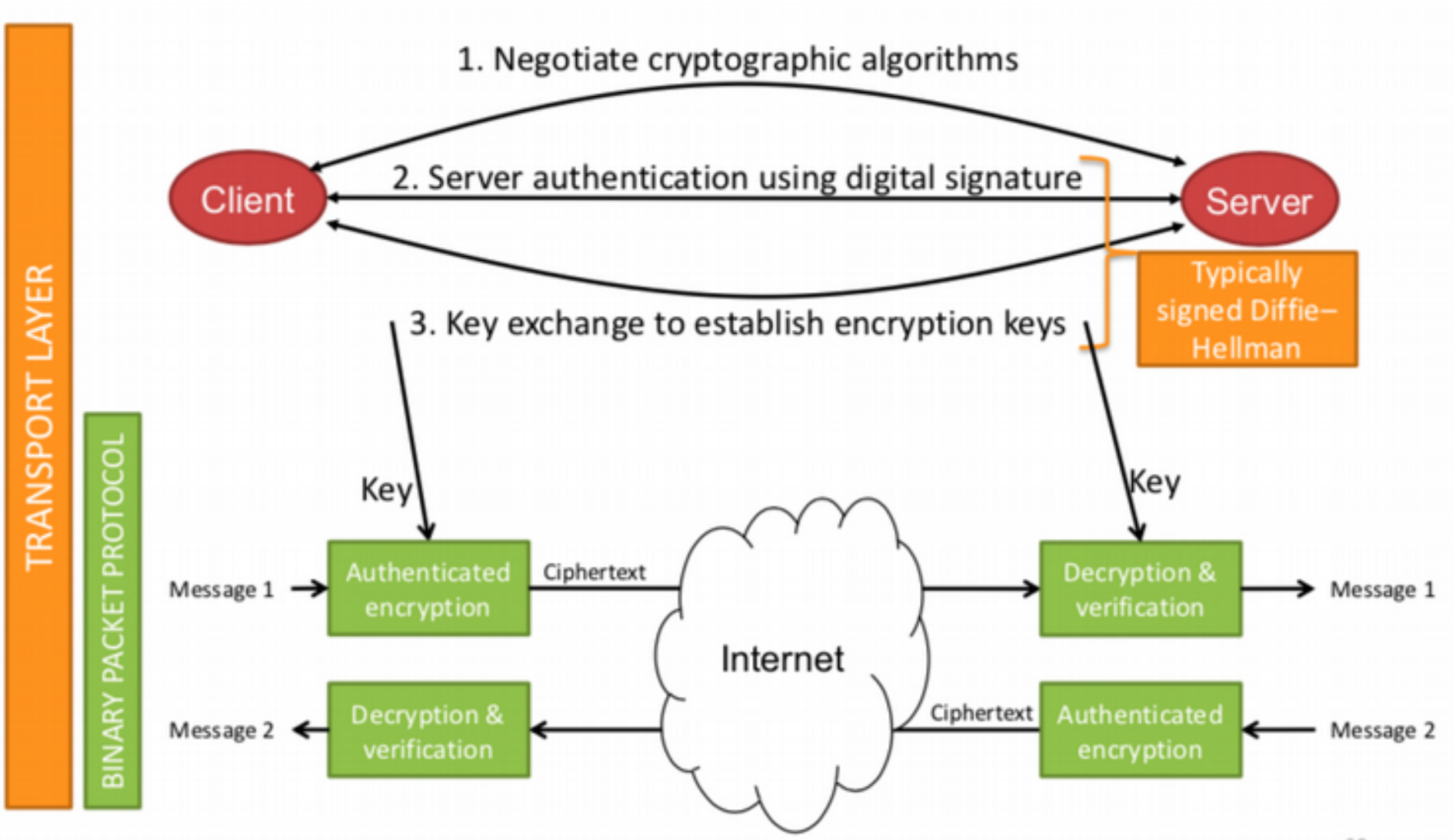
SSH (Secure Shell) Protocol

- SSH used for secure remote access (like telnet, but secure)
- Occasionally used as a"poor man's VPN"
- Run over TCP, typically on port 22
- Provides public key authentication of servers and clients and encrypted communication

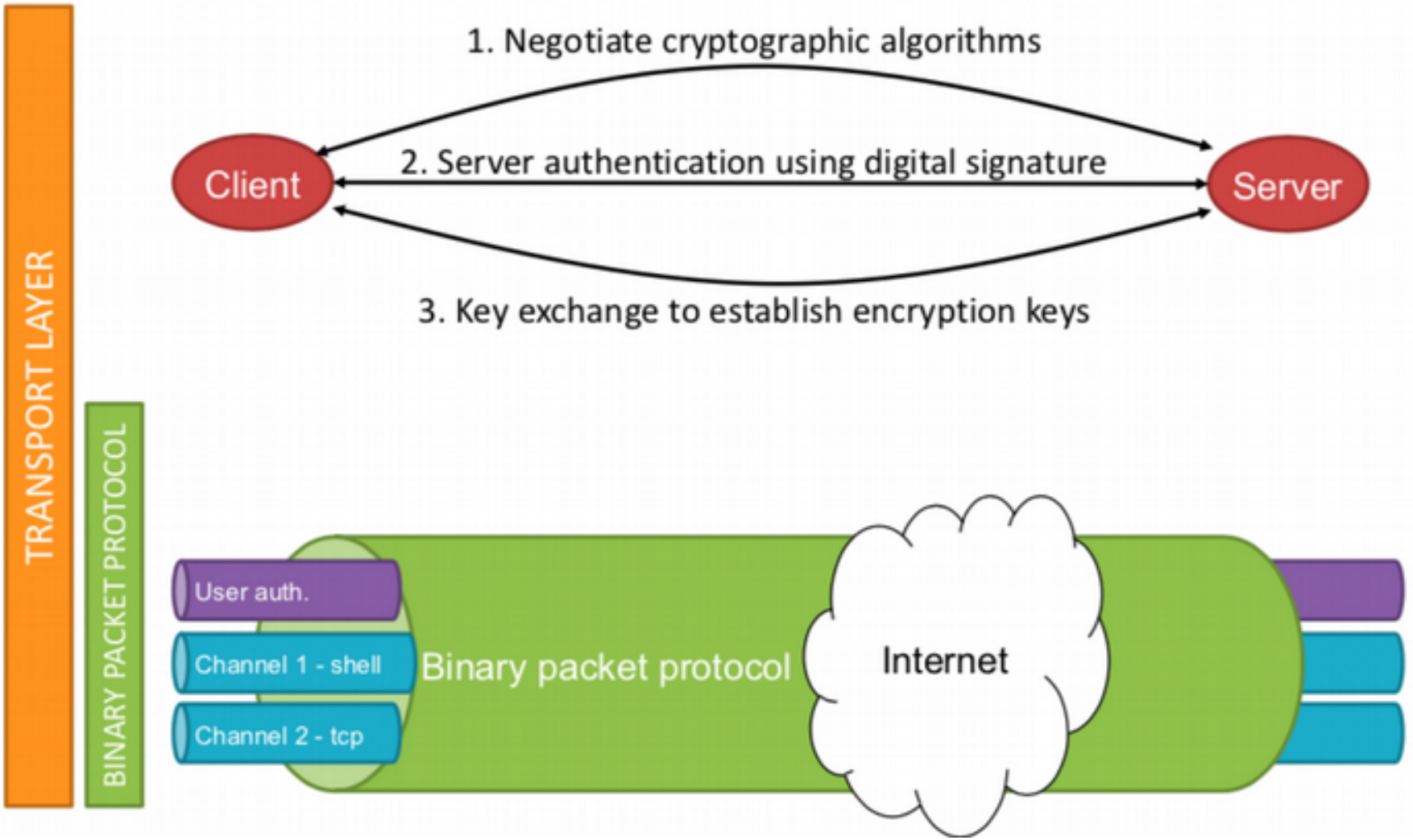
Security Goals of SSH

- **Message Confidentiality**
  - Protects against unauthorised data disclosure
  - Achieved using encryption
- **Message Integrity**
  - Protects against unauthorised changes to data during transmission (intentional or unintentional)
  - Achieved using message authentication code
- **Message Replay Protection**
  - The same data is not delivered multiple times
  - Achieved using counters and integrity protection
- **Peer Authentication**
  - Ensures that traffic is being sent from the expected party
  - Server-to-client auth:
    - based on public keys
  - Client-to-server auth:
    - based on passwords or public keys

SSH (Secure Shell) Protocol



SSH (Secure Shell) Protocol



Server Authentication in SSH

- Based on public key digital signatures
- Unlike TLS, (typically) does not use X.509 certificates – just a raw public key
- No systematic solution for authentic distribution of public keys
  - Console displays public key fingerprint (hash) on first login
  - User should check hash through some out-of-band method
  - SSH client saves hash for future logins and raises alert if changed

Host key verification

If the host is not in the known host list or cannot authenticate the public key found there, one gets a prompt:

```
The authenticity of host 'vm1.cs.yale.edu (128.36.229.150)' can't be established. RSA key fingerprint is c9:a5:be:55:af:ab:05:77:b4:30:62:ed:bd:be:50:43.

Are you sure you want to continue connecting (yes/no)?
```

If you say yes, the public key of that host gets entered into the known hosts and used the next time.

Client Authentication in SSH

- Based on passwords or public key digital signatures
- Security-conscious installation would disable password-based authentication and only support public key authentication

IPsec (Internet Protocol Security)

- Provides confidentiality and authentication for Internet communications
- Works at the IP layer of the protocol stack
  - TLS works at higher levels, so applications have to be designed to use TLS
  - IPsec can be used transparently with any application
- Often used for Virtual Private Networks (VPNs)

IP Security Overview

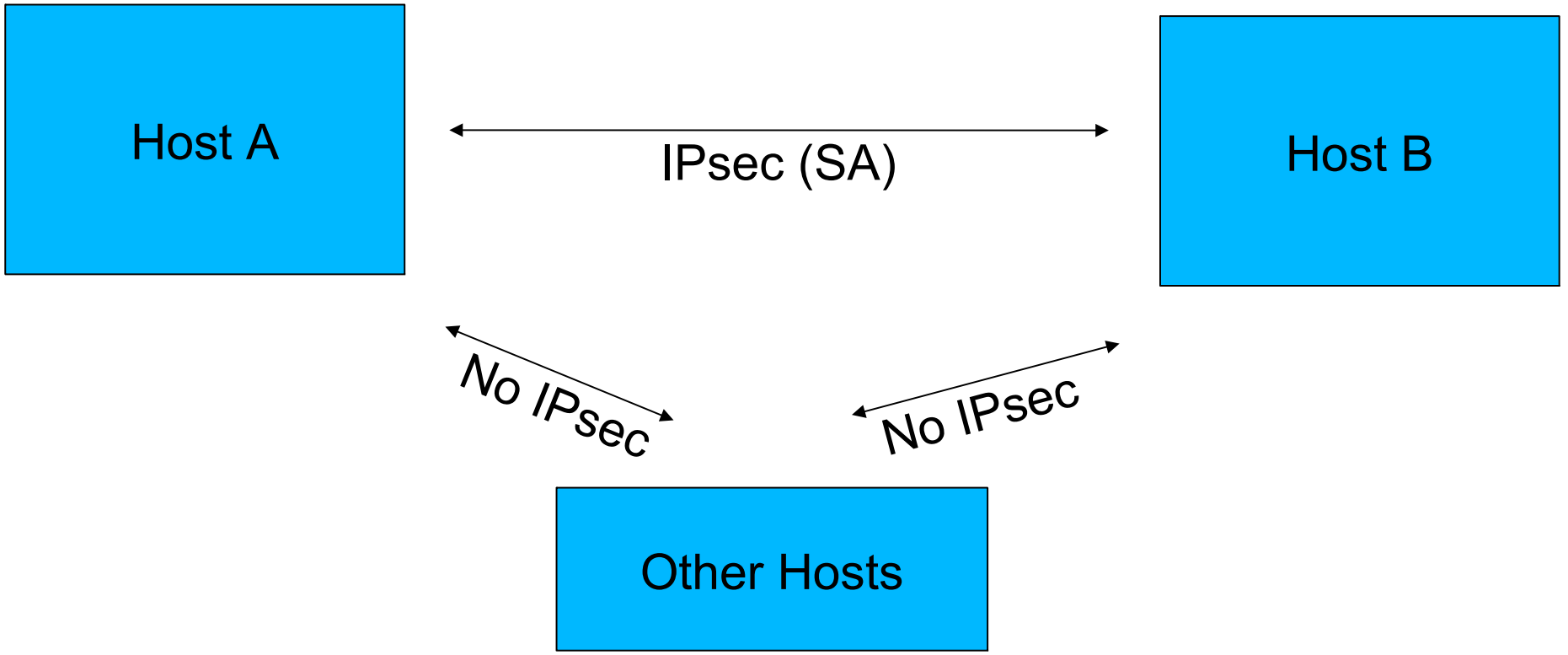
- Benefits of IPSec
  - Transparent to applications (below transport layer (TCP, UDP)
  - Provide security for individual users
- IPSec can assure that:
  - A router or neighbor advertisement comes from an authorized router
  - A redirect message comes from the router to which the initial packet was sent
  - A routing update is not forged

Types of communications

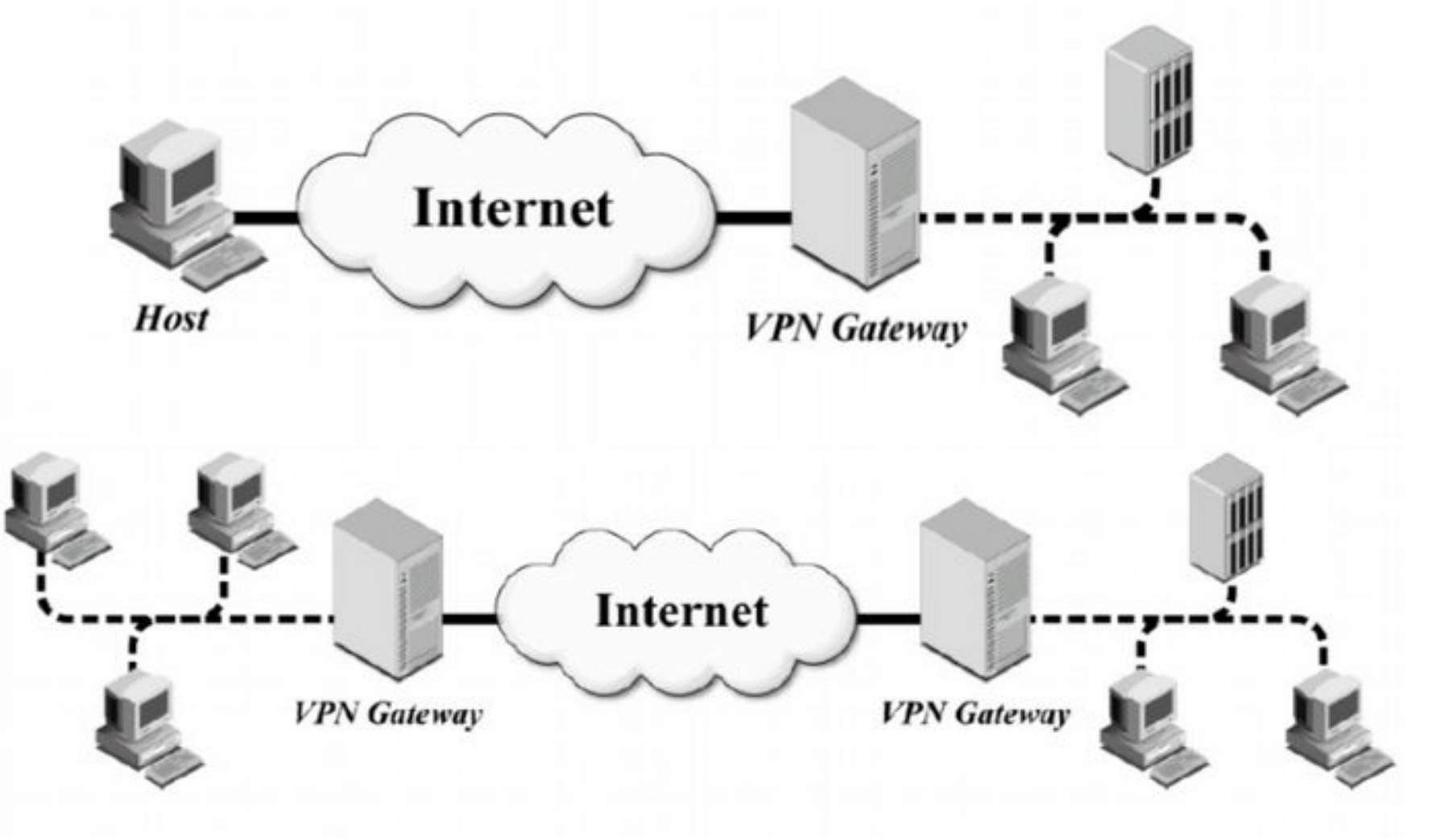
- Host To Host
- Host To Security Gateway
- Security Gateway To Security Gateway
  - Security Gateway = Firewall
  - Also refer to as Network (i.e. Network To Network)

How does IPSEC work?

- Host To Host



Common Architectures



Types of IPSEC Connections

- **Transport Mode**
  - Does not encrypt the entire packet
  - Uses original IP Header
  - Faster
- **Tunnel Mode**
  - Encrypts entire packet including IP Header (ESP)
  - Creates a new IP header
  - Slower

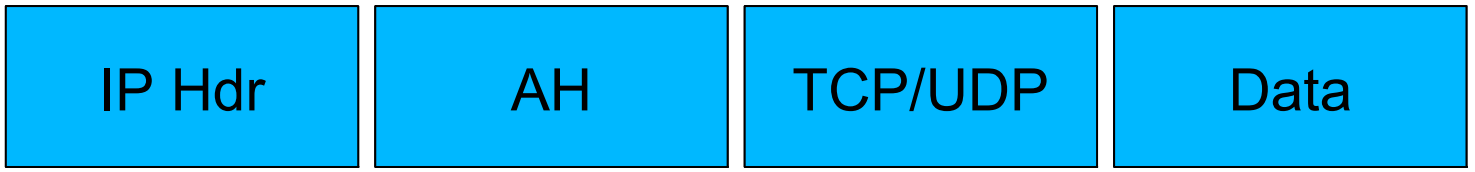
IPSec Headers

- Security extensions for IPv4 and IPv6
- IP Authentication Header (AH)
  - Authentication and integrity of payload and header
- IP Encapsulating Security Protocol (ESP)
  - Confidentiality of payload

AH (Authentication Header)

- IP Protocol 51
- Provides authentication of packets
- Does not encrypt the payload

Transport Mode



Tunnel Mode

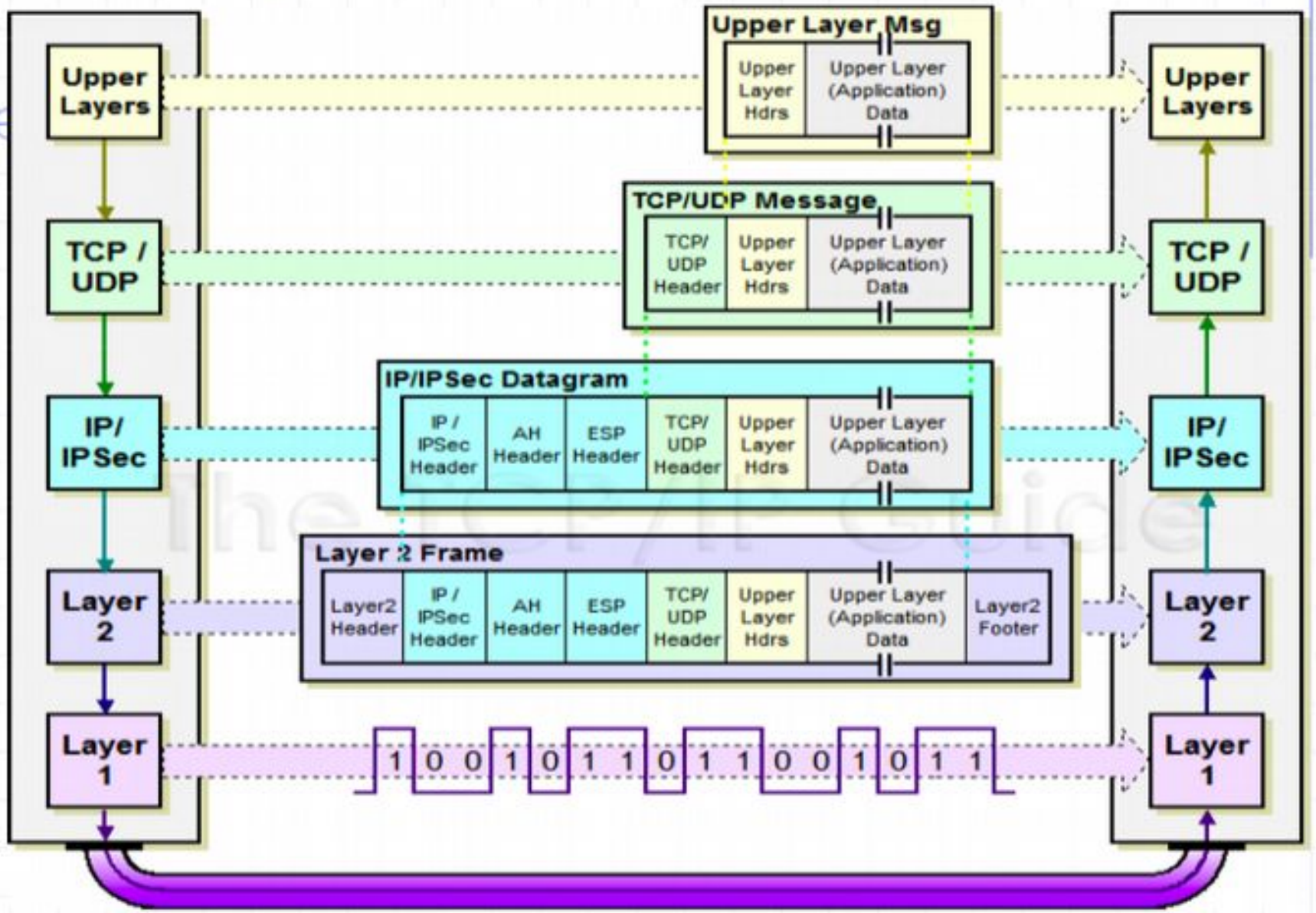
ESP (Encapsulating Security Payload)

- IP Protocol 50
- Encrypts the Payload
- Provides Encryption and Authentication

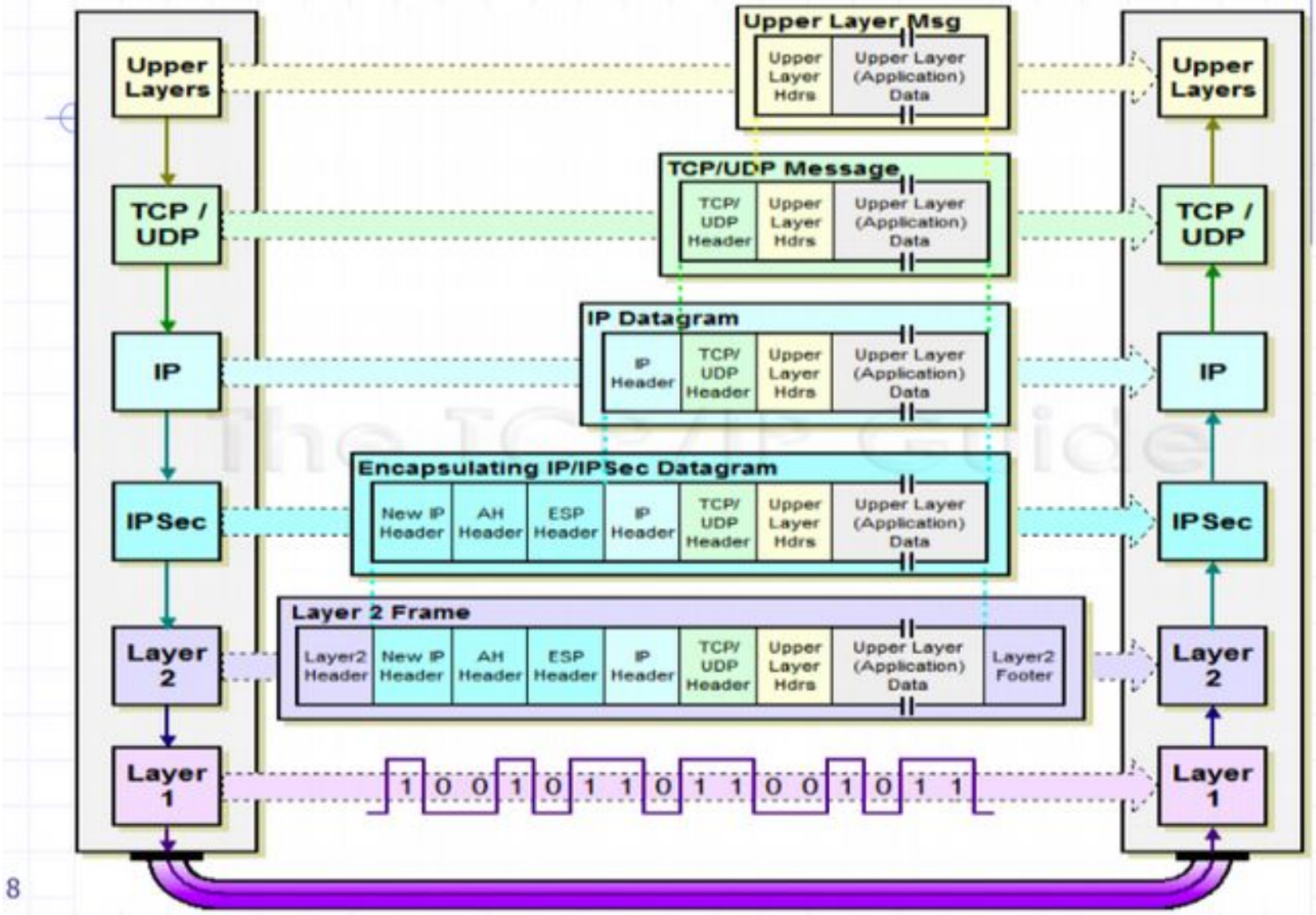
Transport Mode

Tunnel Mode

IPSec Transport Mode: IPSEC instead of IP header



IPSec Tunnel Mode: IPSEC header + IP header



Transport vs Tunnel Mode ESP

- Transport mode is used to encrypt & optionally authenticate IP data
- data protected but header left in clear
- can do traffic analysis but is efficient
- good for ESP host to host traffic
- Tunnel mode encrypts entire IP packet
- add new header for next hop
- good for VPNs, gateway to gateway security

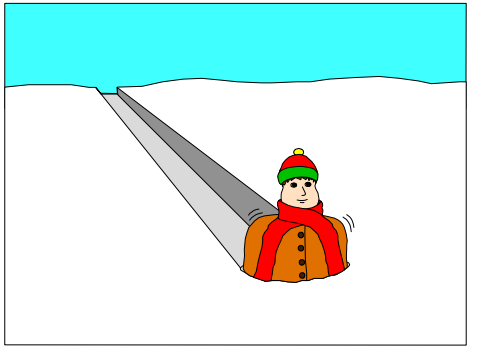
Summary

	Transport Mode	Tunnel Mode
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers	Authenticates entire inner IP packet plus selected portions of outer IP header
ESP	Encrypts IP payload and any IPv6 extension header	Encrypts inner IP packet
ESP with authentication	Encrypts IP payload and any IPv6 extension header. Authenticates IP payload but no IP header	Encrypts inner IP packet. Authenticates inner IP packet.

VPN (Virtual Private Network)

A Virtual Private Network Carries Private Traffic Over a Public Network

- Secure communications between two hosts or networks
- IPsec is one of the more popular VPN technology's



Wireless LAN

IEEE 802.11

- Working group of the IEEE (Institute of Electrical and Electronic Engineers)
- Various standards for WLAN protocols
  - Core OSI layer 1 and layer 2 WLAN standards: 802.11, 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, …
  - Security standards: 802.11i, 802.1X, …

Wi-Fi Alliance

- Trade group that owns the Wi-Fi trademark and licenses it to products that comply with a certain subset of (rebranded) IEEE standards for interoperability
  - ≥ 1 of 802.11 a/b/g/n
  - Wi-Fi Protected Access II (WPA2) ≈ 802.11i

Wireless LAN Security Protocols

	IEEE	Wi-Fi Alliance	
1997	Wired Equivalent Privacy (WEP)	N/A	Included in original 802.11 standard
2003	802.11i draft	Wi-Fi Protected Access (WPA)	
2004	802.11i	Wi-Fi Protected Access II (WPA2)	
2001–2004	802.1X	WPA-Enterprise WPA2-Enterprise	
2006	N/A	Wi-Fi Protected Setup (WPS)	

Wired Equivalent Privacy (WEP)

- **Entity Authentication:**
  - Open System authentication:
  - Basically no authentication
  - Ethernet MAC address – easily spoofed – Shared Key authentication:
  - Challenge-response protocol based on knowledge of pre-shared key

- **Confidentiality & Integrity:**
  - Encryption using RC4 with various key sizes – Integrity using CRC-32 checksum

Wi-Fi Protected Access (WPA2)

- Wi-Fi Alliance name for the IEEE 802.11i final standard of 2014

- **Entity Authentication:**
  - WPA-Personal, WPA-Enterprise, Wi-Fi Protected Setup

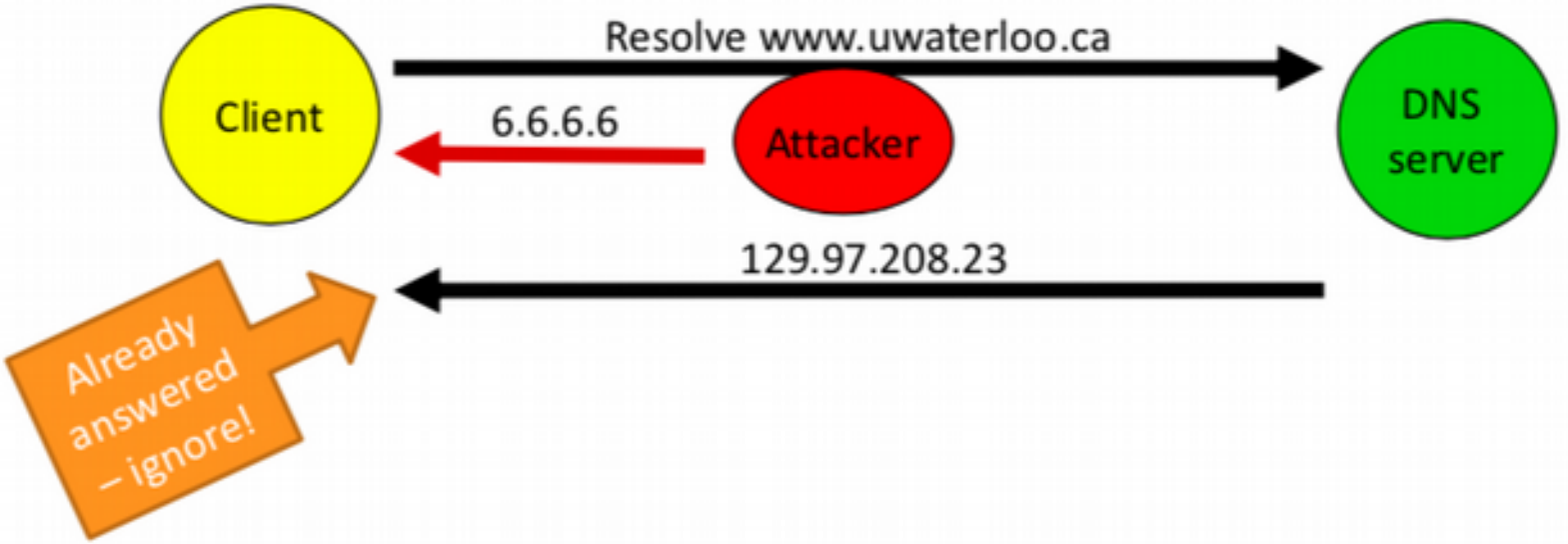
- **Confidentiality & Integrity:**
  - Encryption: AES in Counter Mode
  - Integrity: AES-CBC-MAC

Domain Name System (DNS)

- Hierarchical directory service for domain names
- Main feature: translates domain names into IP addresses
- A domain name record can provide a variety of additional information
  - Authorized name servers – Mail server addresses
  - Anti-spam information
  - Public keys

Attacks

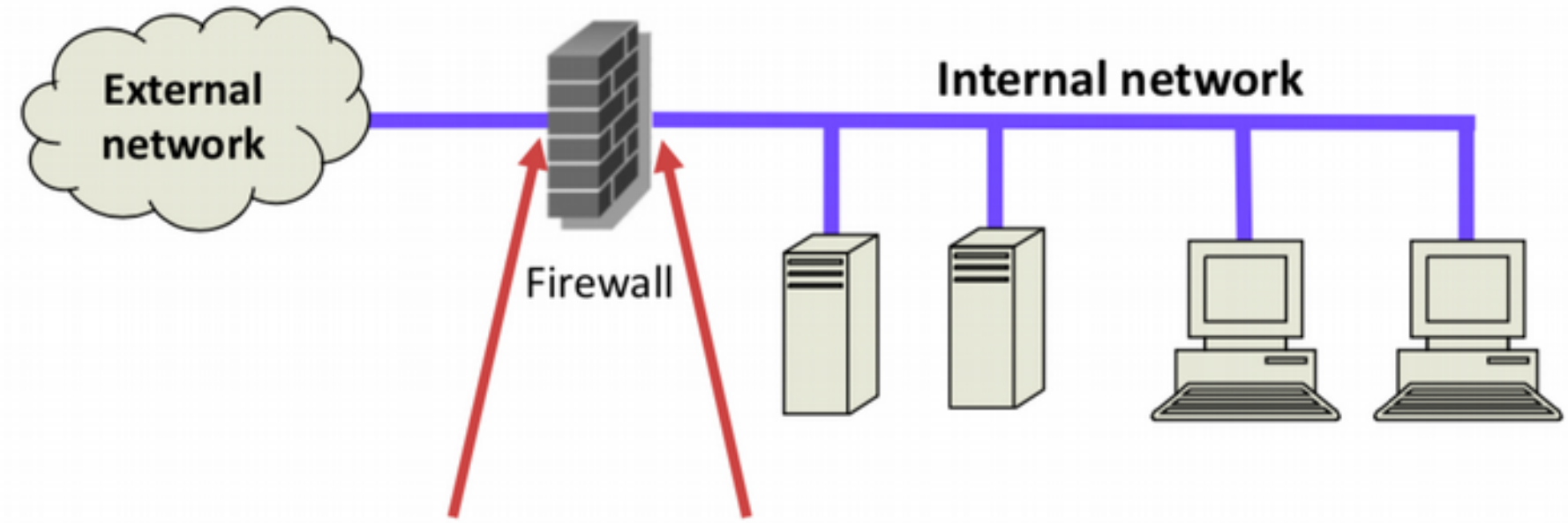
- Goal: Spoof responses to DNS queries to redirect queries for a particular domain name to attacker-controlled IP address



DNSSec

- DNS Security Extensions uses digital signatures to protect DNS records
- The DNS root is the trusted party
- The signature chain is built from the DNS root to the current subdomain
- Not so easy to design a backward-compatible standard that can scale to the size of the Internet
- Many feel their DNS info is confidential
- DNSSEC deployment is complex

Firewall



Firewall has two network interfaces:
One for external traffic, one for internal traffic

Firewall Policies

- Enforce a security policy established by an administrator on all network traffic passing the boundary
- Two policy approaches:
  - **Default permit:** allow all traffic except that which is expressly prohibited (blacklist)
  - **Default deny:** block all traffic except that which is expressly permitted (whitelist)

Packet Filters

- Operate at the network or transport layer
- Makes decisions based on information in packet headers, such as
  - IP headers: source or destination IP address
  - Protocol: TCP, UDP, or ICMP
  - TCP headers: source or destination port numbers
  - Direction of travel (into/out of the internal network)

Stateless Packet Filters

Stateless: Examine each packet independently of other packets

- Even if they are part of the same connection
  - High speed
  - Low memory

Stateful Packet Filters

- Stateful packet filters operate in the same way as stateless packet filters:
  - examining headers and comparing to ruleset to see if the packet transmission is allowed under the firewall rules
- But stateful packet filters also keep a state table noting the state of each connection:
  - Is the connection being established, in use, or terminated?
- Stateful packet filters examine the state in the context
  - If header values contradict the expected state, the packet will be dropped

Application-level Gateway (proxy)

- Use an application specific gateway/proxy
- Has full access to protocol
  - User requests service from proxy
  - Proxy validates request as legal
  - Then forwards request and returns result to user
- Need separate proxies for each service
  - some services naturally support proxying
  - others are more problematic
  - custom services generally not supported
  - Ex: HTTP for Web

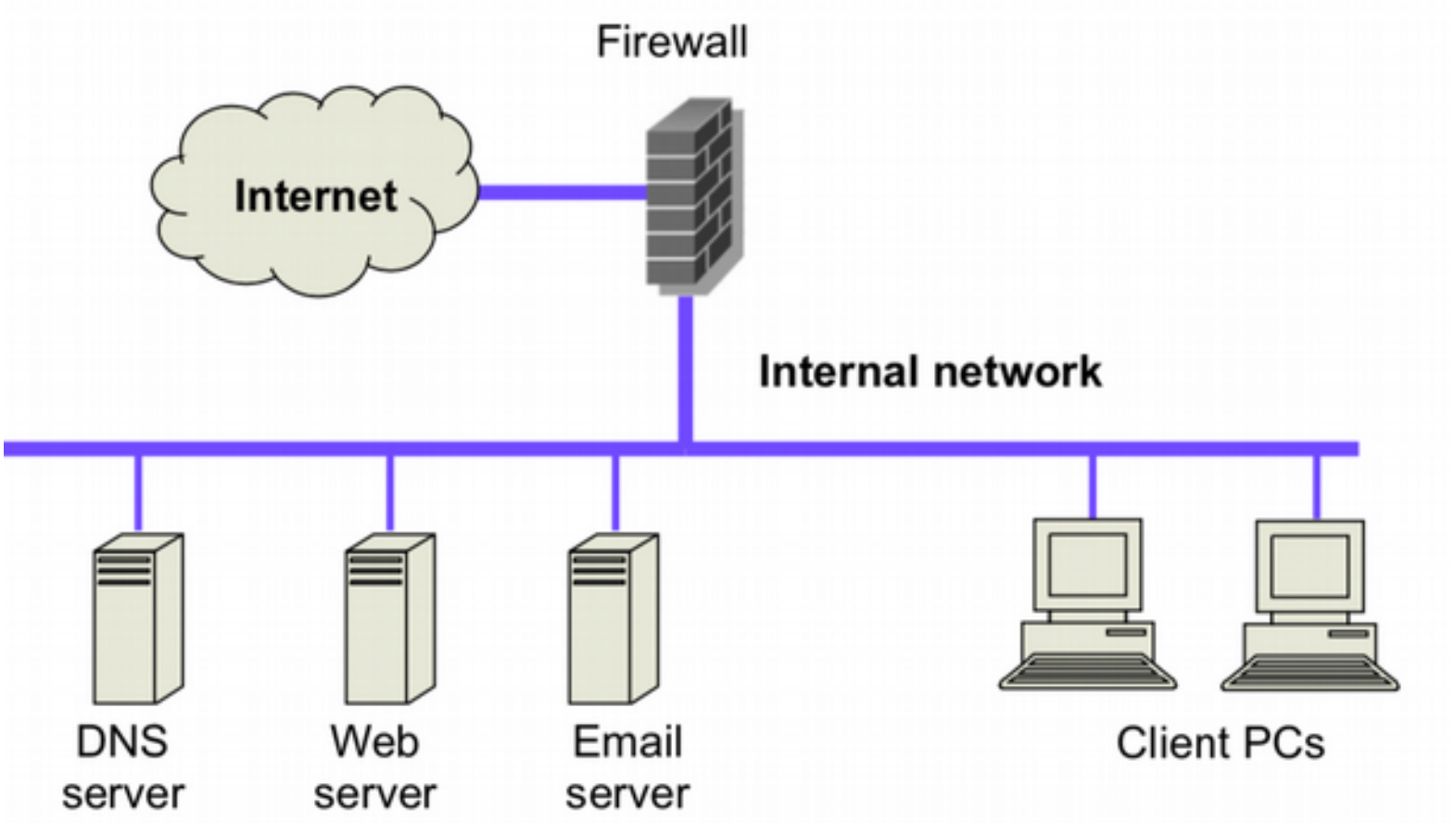
    FTP for file transfers

    SMTP/POP3 for e-mail

Comparing Firewall Types

Stateless packet filter	Stateful packet filter	Application proxy
Inspects single packets	Tracks state across many packets	Tracks state across many packets
Examines IP and TCP headers	Examines IP and TCP headers	Examines application data
High speed	Medium speed	Low speed
Simplest rules	Simple rules	Complex rules
Little/no auditing/logging	Auditing/logging possible	Auditing/logging likely

Simple Firewall Architecture



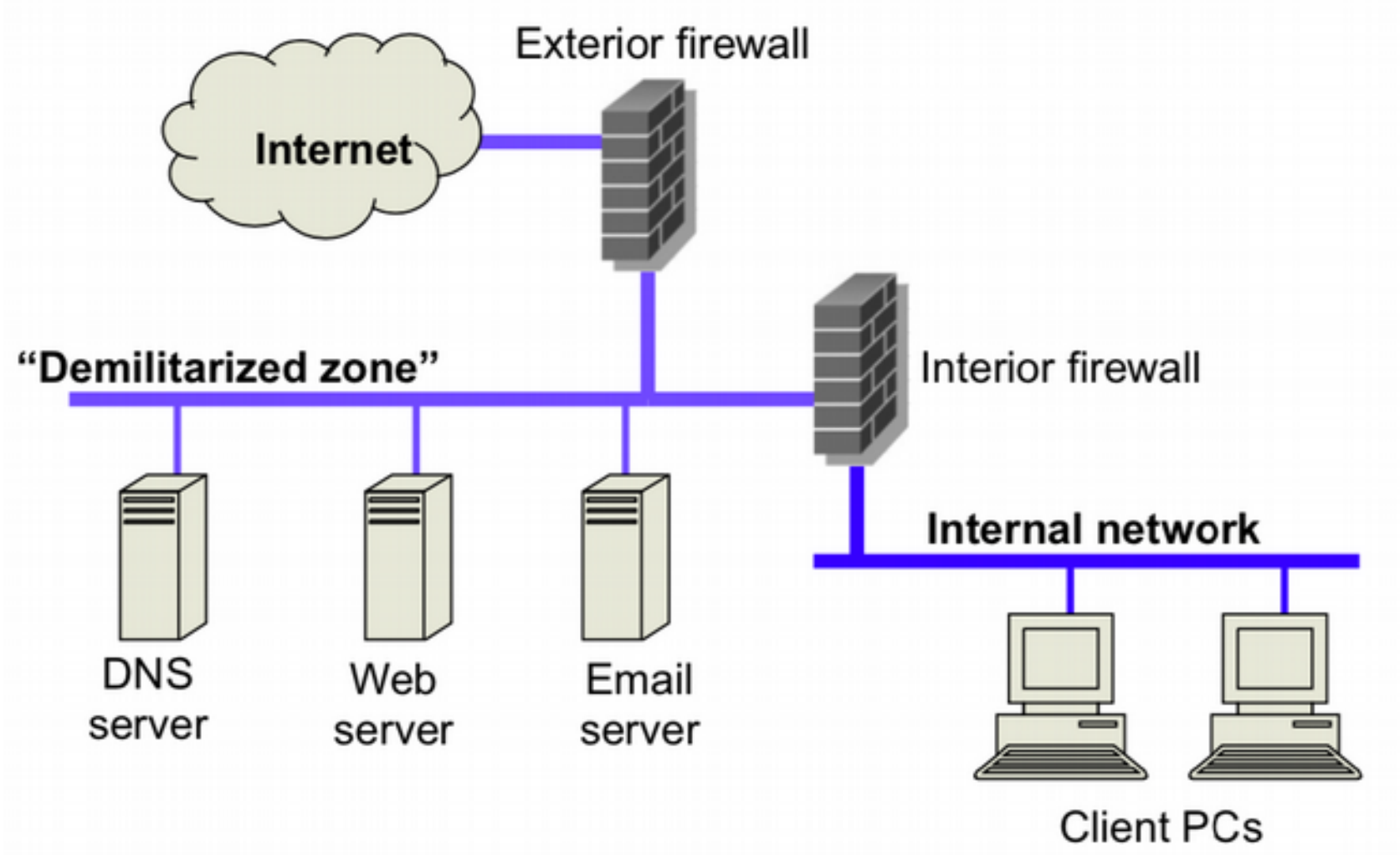
Features and Functionality

- A wide range of additional features and functionalities are being integrated into standard firewall products.

These are

- Demilitarized zone (DMZ)
- Content filtering
- Virtual private networking (VPN).

DMZ Firewall Architecture



Personal Firewalls

- A personal firewall is a software program that is designed to protect the computer on which it is installed.
- Frequently used by home users to provide protection against unwanted Internet traffic.
- Usually these are stateful packet filters

- Examples:
  - Windows, Ubuntu, and macOS all include a personal firewall
  - Commercial personal firewalls: ZoneAlarm, Symantec, Little Snitch, ...
  - Some include anti-virus software as well

Technical Challenges with Firewalls

- Simple Packet Filter:
  - Have high performance
  - do not do any content-based filtering: if email is allowed through, then emails containing viruses or malicious codes are allowed through.
- Application level gateways offer more comprehensive filtering
  - Hard to configure; policy errors are common
  - Need to be kept up to date
  - Often ways to bypass

Technical Challenges with Firewalls

- Some services don't work, because they're blocked.
- Network diagnostics may be harder.
- Encrypted traffic cannot be examined or filtered

  https, ssh, etc.
- Firewalls, VPN, and NAT together can cause confusion or compromise security.

Non-Technical Challenges with Firewalls

- Rely on well-formulated security policy
- Perimeter security is often bypassed
- Training human operators
- **Firewall != Security**

Intrusion Detection System (IDS)

- Intrusion detection is the process of identifying and responding to malicious activity targeted at resources
- IDS uses collected information and predefined knowledge-based system to reason about the possibility of an intrusion.
- IDS also provides services to cop with intrusion such as giving alarms, activating programs to try to deal with intrusion, etc.

NIDS

- A Network-based IDS system examines the individual packets flowing through a network and should be able to understand all the different flags and options that can exist within a network packet.
- It can then detect malicious packets (that may be overlooked by firewalls' rules).
- It can also look at packet payload, (try to understand what program is being accessed and with what options).

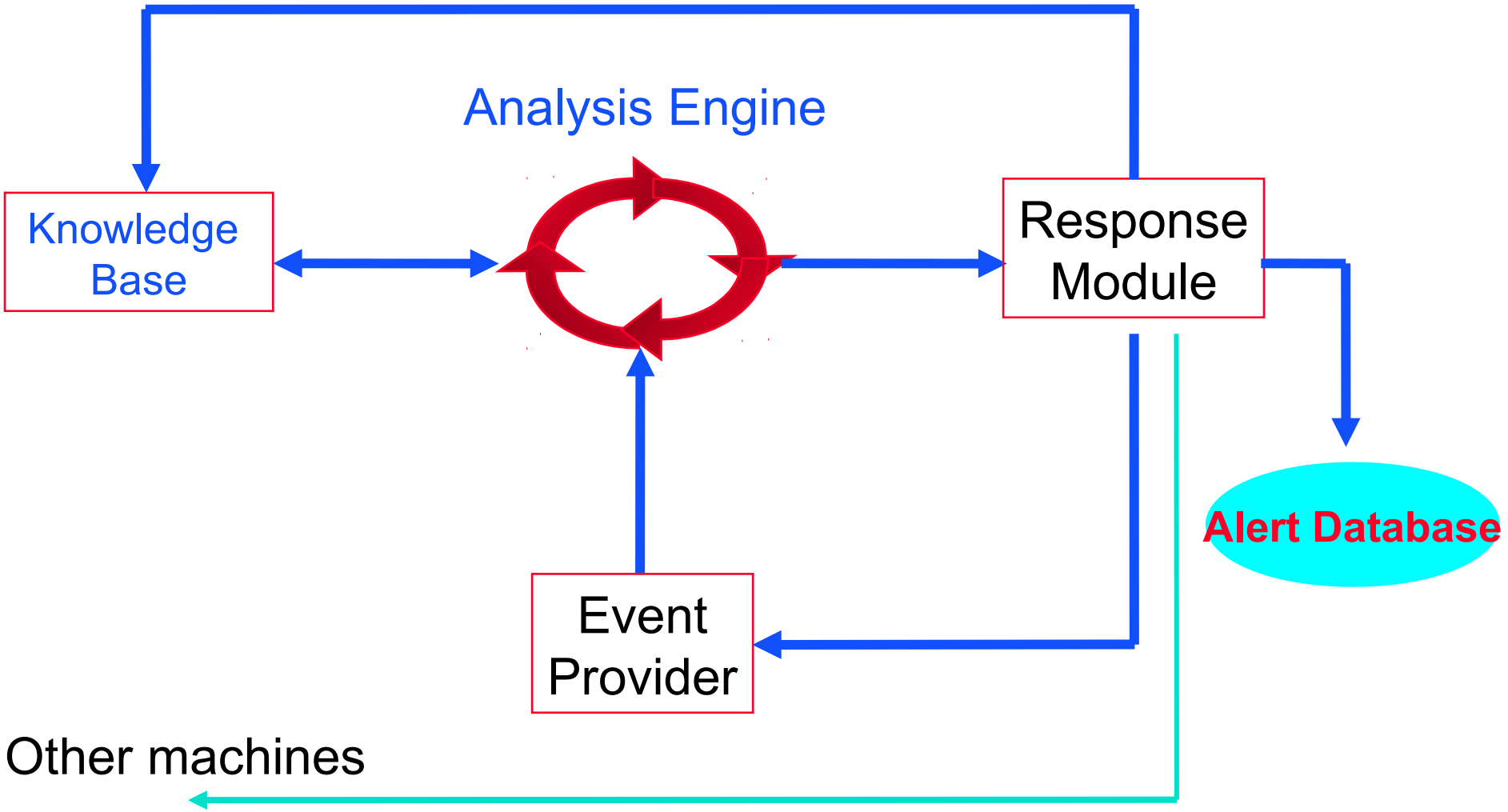
HIDS

- A Host based IDS system – examines activity on individual computers (hosts). It can detect repeatedly failed access attempts or changes to the local's critical system files.

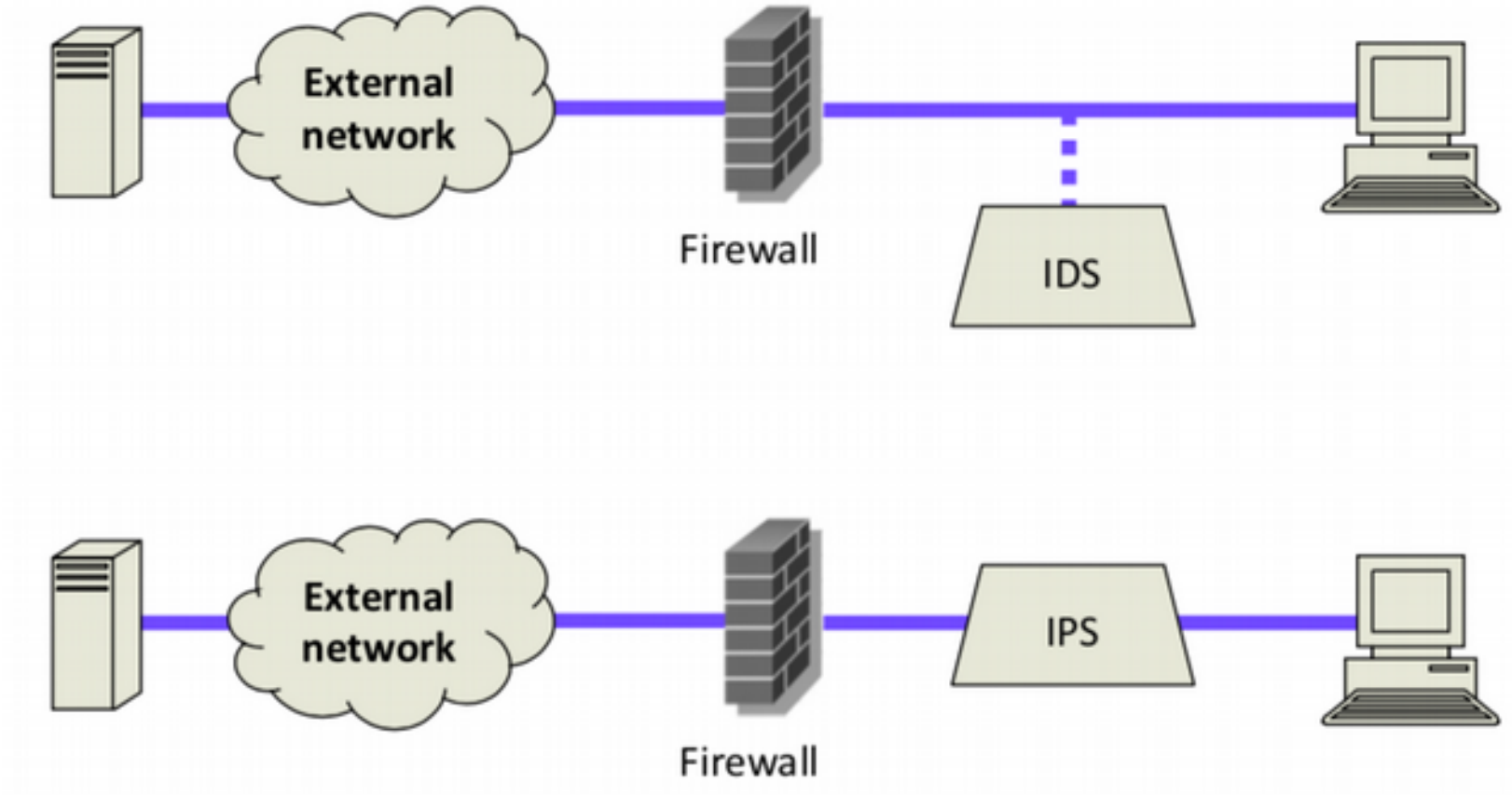
HIDS versus NIDS

- HIDS can monitor user-specific activity of the system
- Check process listing, local log files, system calls.
- It is difficult for NIDS to associate packets to specific users and to determine if the commands in the packets violate specific user's access privilege.
- HIDS can help detect attacks that can escape from NIDS detection.
- HIDS sensor can monitor encrypted traffic by tapping in at the connection endpoint such as VPN connection.
- But NIDS can not check encrypted packets such as encrypted IPSec/SSL payload.
- NIDS can detect such as DOS and port scan that HIDS cannot.
- NIDS can detect attacks to main targets in DMZ such as Web servers, mail servers, etc. to minimize damages.
- Without NIDS in place, it is hard to determine if the network has been attacked or not.

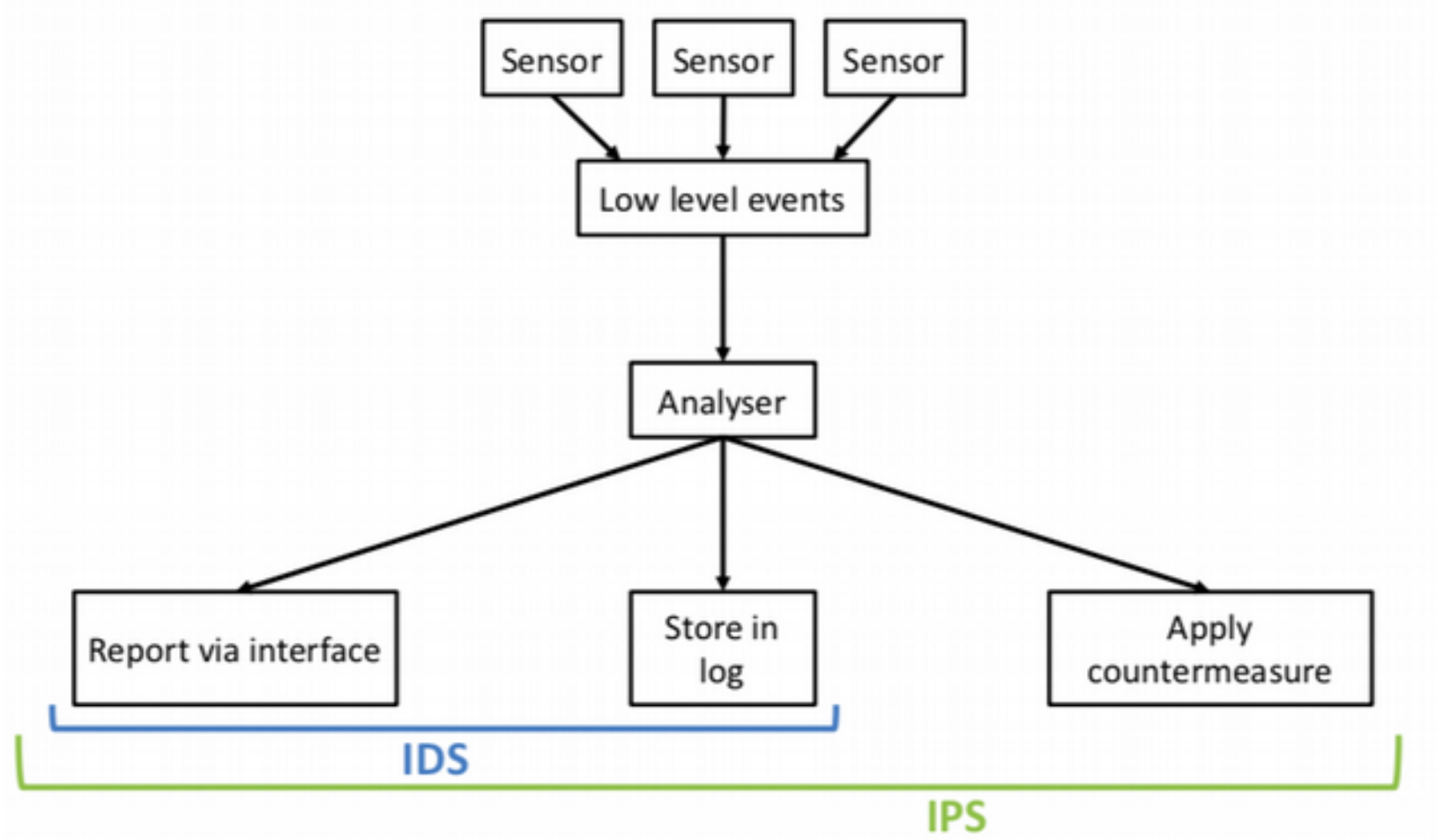
Intrusion Detection System (IDS)



IDS and IPS


External network
Firewall
IDS
External network
Firewall
IPS

Model of IDS / IPS



Types of Analyses

Signature- or misuse-based detection

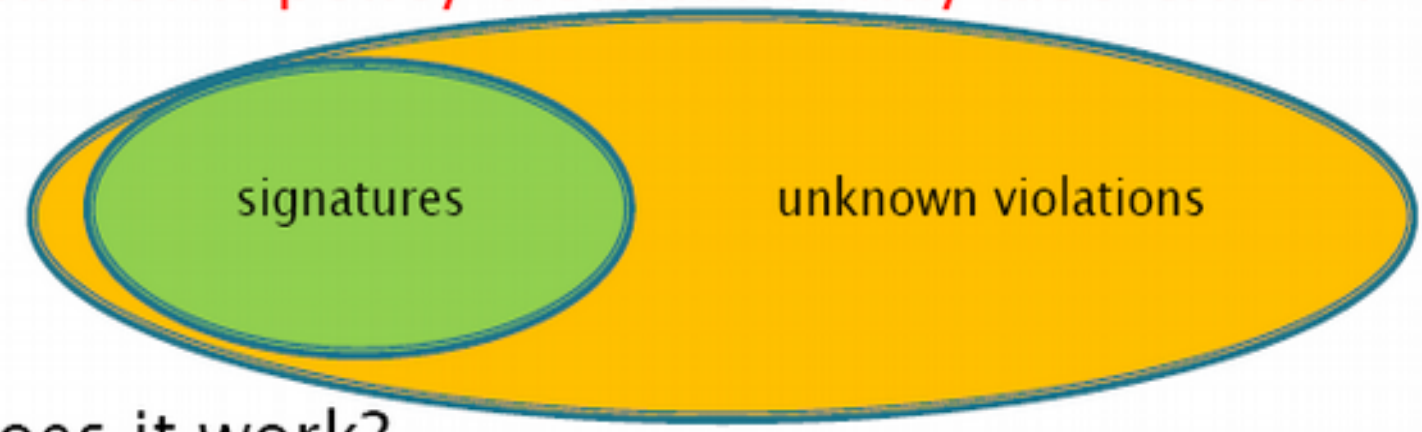
- detects pattern or signature matching known misuse or threat

Anomaly- or heuristic-based detection

- detects deviation from normal
  - Network Behaviour Analysis
  - Stateful Protocol Analysis

Detection system: signature based

- Well-known example: anti-virus
- Uses known policy violations for detection
- Policy violation → alert
- Frequent updates required in most cases
- Unknown policy violations may also exist…



- Does it work?

Detection system: anomaly based

- Well-known example: credit card fraud teams
- Uses known good behavior
- Behavior not good → alert
- Good behavior must be known first
  - What happens if your mom uses your computer?
- Does it work?

Limitations of Analysis Types

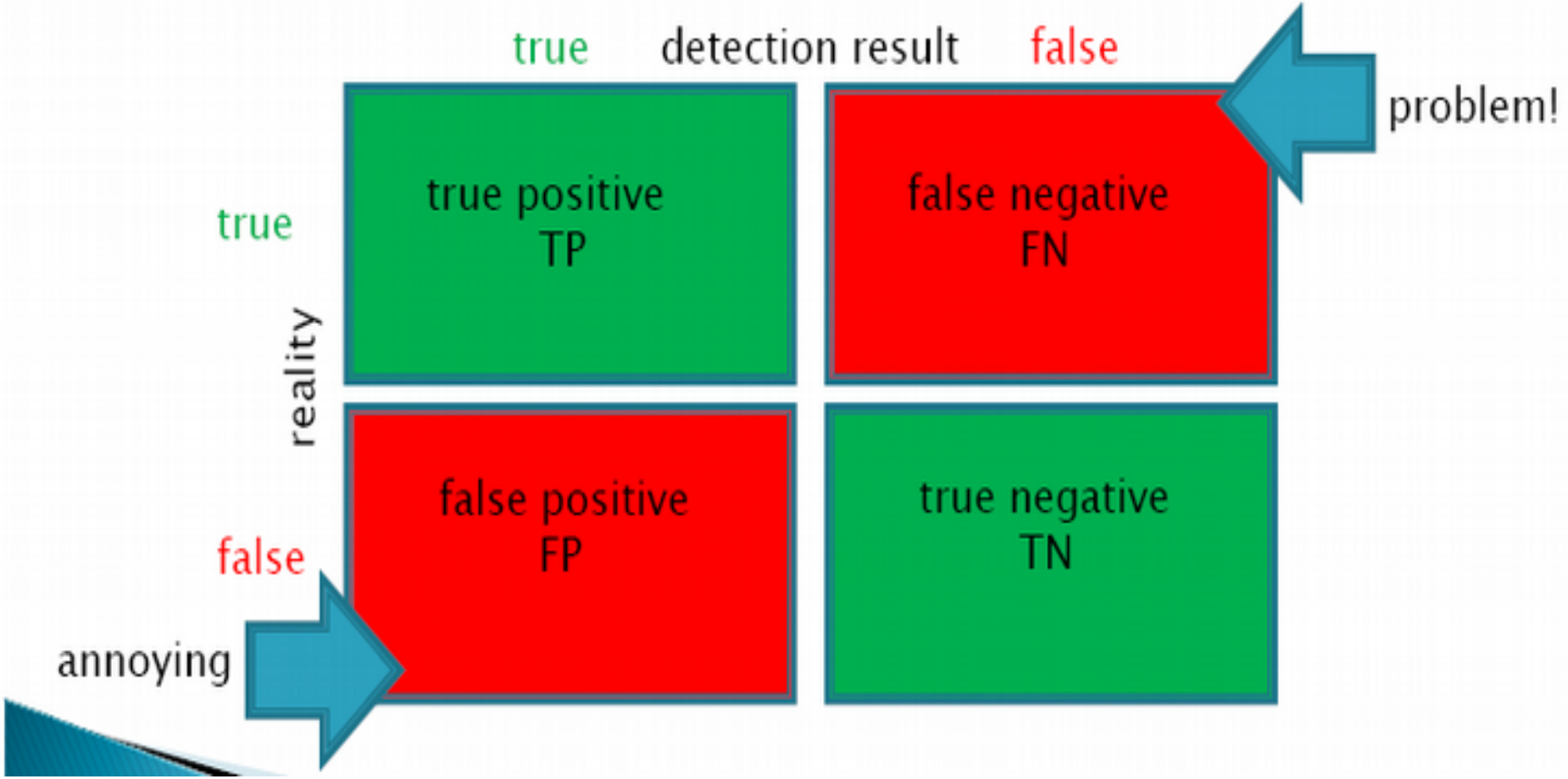
Signature- or misuse-based detection

- Ineffective against novel (zero-day) attacks where misuse pattern is unknown
- Ineffective against polymorphic attack code

Anomaly-based detection

- Requires training or learning “normal” profile
- High false-positive rate

Effectiveness



We want 100% TP (= 0% FP), 100% TN (= 0% FN)

HIDS and NIDS: Example

- Host-based IDS:
  - Periodically analyse logs, perform file system integrity check. Eg:
    - Generic: Real Secure Server Sensor.
    - Check host file system: OSSEC, Tripwire, AIDE (advanced Intrusion Detection Environment).
- Network-based IDS:
  - Analyse network traffic contents and patterns for signs of intrusion
  - Examples:
    - Snort and Cisco IDS.

www.ossec.net

www.snort.org

Firewalls vs. IDS vs. IPS

Packet filter	Application proxy	IDS	IPS
Preventive	Preventive	Detective	Preventive
Examines packet headers		Examines packet headers	Examines packet headers
	Examines application data	Examines application data	Examines application data
Drops packets not matching policy	Drops packets not matching policy		Drops packets not matching policy
		Logs / raises alerts for data matching criteria	Logs / raises alerts for data matching criteria
			Applies countermeasures

Simple, fast ⟷ Complex, slow

Discussion